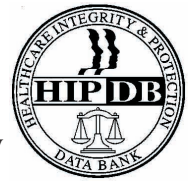# National Practitioner Data Bank
Healthcare Integrity and Protection Data Bank
P.O. Box 10832, Chantilly, Virginia 20153-0832 • www.npdb-hipdb.hrsa.gov

FACT SHEET ON USER IDs AND PASSWORDS

Internet Querying and Reporting

Registered entities with active querying and reporting privileges and authorized agents on behalf of registered entities use the Integrated Querying and Reporting Service (IQRS) to query and/or report to the National Practitioner Data Bank (NPDB) and the Healthcare Integrity and Protection Data Bank (HIPDB). The IQRS is an electronic, Web-based system that represents part of an ongoing effort to improve the efficiency and responsiveness of the NPDB-HIPDB.

The IQRS allows for reporting and querying to the Data Bank(s) through the Internet. The NPDB-HIPDB does not accept queries or reports submitted on paper.

For information about IQRS security features, system requirements, and instructions for use, see the *Fact Sheet on the Integrated Querying and Reporting Service (IQRS)*.

Logging In to the IQRS

The IQRS *Login* screen (Figure 1) has three fields that must be completed to access the IQRS. Enter your Data Bank Identification Number (DBID), User ID, and User Password into the corresponding fields and click **Login**. The User Password and User ID fields are case sensitive. Enter your login information exactly as it appears on the *Entity Registration Verification* document that was mailed to you after your entity registered successfully.
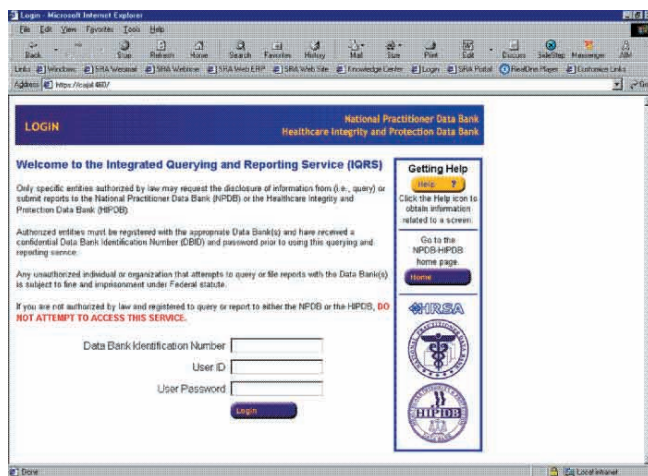

Figure 1. Login Screen

Creating and Maintaining User Accounts

Every entity must maintain an administrator account. If your entity has only one person who uses the IQRS, you may choose to use the administrator account as your regular user account. The administrator account is the only account that may create, edit, and delete other user accounts for the entity. Entities may have an unlimited number of additional user accounts.

To modify a user account, the administrator selects **Maintain User Accounts** on the *Administrator Options* screen to display the *Maintain User Account* screen. Only the administrator can access the *Maintain User Account* screen (Figure 2).

To create a new user account, click **Add** on the *Maintain User Account* screen. The *User Account Information* screen displays, where the administrator may add information on a new user.
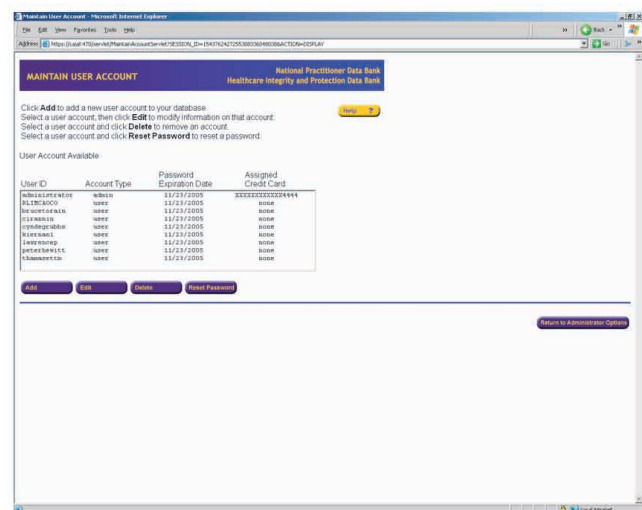

Figure 2. Maintain User Account Screen

User IDs

All user IDs have the following characteristics:

• They must contain at least eight characters.
• They must contain only alphanumeric characters.
• They are case sensitive.
• They must be unique for the entity user.

To remove a user account, highlight the user's account information on the *Maintain User Account* screen and select **Delete**. The account is removed immediately.

To reset a user password, highlight the user's account information on the *Maintain User Account* screen, select **Reset Password**, and follow the on-screen instructions.

To edit a user account, highlight the user's account information on the *Maintain User Account* screen and click **Edit.** The *User Account Information* screen (Figure 3) displays, where the administrator may change the user's Password, Name, Title, Telephone, E-mail, and Street Address. (Non-administrator users may also access the *User Account Information* screen and update their own password and other information by selecting **Update User Account** on the *Options* screen.)

Figure 3. User Account Information Screen

User Passwords

The administrator must also create a password for each new user ID. As with all other IQRS transactions, passwords are sent through a secure server to the NPDB-HIPDB. Passwords must comply with the following requirements:

•   They must contain at least eight characters.

•   They must contain a combination of alphanumeric characters.

•   They are case sensitive.

•   They must contain at least one number.

•   They must not contain a word found in the dictionary.

•   They must not be your User ID.

•   They must not be a common Data Bank phrase (e.g., NPDB, IQRS).

•   They must not be a simplistic or systematic sequence (e.g., abcd1234).

Passwords may also include any of the following characters: **!@#$^&*( )-_=+[ ] { } | ;:,.< >?.**

Passwords are valid for 90 days. The expiration dates for all user passwords may be viewed by the administrator on the *Maintain User Account* screen. After 90 days, users must change their passwords. The system will ensure that the new password is different from the previous four passwords used for that user ID. The system will prompt the user 5 days before the password expires. If the user does not change his or her password before it

expires, one grace login will be provided, which can be used up to 30 calendar days after the password expiration. At the grace login, a warning message indicates that the password must be changed immediately; otherwise, the password will expire and future IQRS access will be denied.

Users who forget their passwords or have expired passwords should contact their entity administrator to reset their passwords to a temporary password. Administrators who forget their passwords or have expired passwords must call the NPDB-HIPDB Customer Service Center at 1-800-767-6732 for assistance with obtaining a temporary password.

Procedures for Authorized Agents

If you are an authorized agent with no querying or reporting privileges of your own, you must follow different procedures to update passwords and create user accounts. After logging into the IQRS, the *Agent Registration Confirmation* screen displays and requires you to select your desired role: **Agent Acting on Behalf of Entity With DBID** or **Entity Acting on Behalf of Itself**. In the text box, enter the DBID of an entity that designated you as its authorized agent, then click **Agent Acting on Behalf of Entity With DBID**. The *Entity Registration Confirmation* screen displays with information about the entity whose DBID was entered on the previous screen. Click **Maintain User Accounts** on the *Administrator Options* screen. Changing your password and/or creating user accounts will not affect the entity whose DBID was entered on the *Agent Registration Confirmation* screen. It will modify only your access information.

IQRS Security

The IQRS operates on a secure Web server and uses the latest technology, along with various implementation measures, to provide a secure environment for querying, reporting, data storage, and retrieval. Security features include the following:

•   Firewall protection from unauthorized access.

•   Encryption of transmitted data to prevent unauthorized use.

•   Unique passwords for data entry and retrieval.

•   Multiple unique User IDs to allow entities with multiple departments/people to use the same DBID for querying and reporting, overseen by a single administrator account that can add, update, or remove any of the user accounts.

NPDB-HIPDB Assistance

For additional information, visit the NPDB-HIPDB Web site at *www.npdb-hipdb.hrsa.gov*. If you need assistance, contact the NPDB-HIPDB Customer Service Center by e-mail at *npdb-hipdb@sra.com* or by phone at 1-800-767-6732 (TDD 703-802-9395). Information Specialists are available to speak with you weekdays from 8:30 a.m. to 6:00 p.m. (5:30 p.m. on Fridays) Eastern Time. The NPDB-HIPDB Customer Service Center is closed on all Federal holidays.